IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	)	
	)	
v.	)	Criminal No. 13-243
SEAN TIERNAN	)	

GOVERNMENT'S SENTENCING MEMORANDUM

Defendant Sean Tiernan engaged in a sophisticated scheme in which he compromised tens of thousands of Facebook accounts in order to hijack the usage of other's computing power. This hijacked computing power was then improperly used to send massive amounts of spam messages over the Internet resulting in the Defendant's monetary benefit.

The Third Circuit has set forth a three-step process which the district courts must follow in compliance with the Supreme Court's ruling in United States v. Booker, 543 U.S. 220 (2005):

(1) Courts must continue to calculate a Defendant's Guidelines sentence precisely as they would have before Booker.

(2) In doing so, they must formally rule on the motions of both parties and state on the record whether they are granting a departure and how that departure affects the Guidelines calculation, and take into account our Circuit's pre-Booker case law, which continues to have advisory force.

(3) Finally, they are to exercise their discretion by considering the relevant § 3553(a) factors in setting the sentence they impose regardless whether it varies from the sentence calculated under the Guidelines.

United States v. Gunter, 462 F.3d 237, 247 (3d Cir. 2006) (quotation marks, brackets, and citations omitted) (citing United States v. King, 454 F.3d 187, 194, 196 (3d Cir.2006); United States v.

Cooper, 437 F.3d 324, 329-30 (3d Cir. 2006)). See also United States v. Smalley, 2008 WL 540253, *2 (3d Cir. Feb. 29, 2008) (stating that the Gunter directive is consistent with later Supreme Court decisions). In calculating the guideline range, this Court must make findings pertinent to the guideline calculation by applying the preponderance of the evidence standard, in the same fashion as was employed prior to the Booker decision. United States v. Grier, 475 F.3d 556 (3d Cir. 2007) (en banc). The failure to properly calculate the advisory guideline range will rarely be harmless error. United States v. Langford, 2008 WL 466158, *8-11 (3d Cir. Feb. 22, 2008).

At the third step of the sentencing process, the Court must consider the advisory guideline range along with all the pertinent considerations of sentencing outlined in 18 U.S.C. § 3553(a) in determining the final sentence. "The record must demonstrate the trial court gave meaningful consideration to the § 3553(a) factors. . . . [A] rote statement of the § 3553(a) factors should not suffice if at sentencing either the Defendant or the prosecution properly raises 'a ground of recognized legal merit (provided it has a factual basis)' and the court fails to address it." Cooper, 437 F.3d at 329. See also Rita v. United States, 127 S. Ct. 2456, 2468 (2007) ("The sentencing judge should set forth enough to satisfy the appellate court that he has considered the parties' arguments and has a reasoned basis for exercising his own legal decisionmaking authority."); United States v. Schweitzer, 454 F.3d 197, 205-06 (3d Cir. 2006).

The government explains below its view of the proper consideration in this case of the advisory guideline range and of the Section 3553(a) factors.

I. BACKGROUND

On November 5, 2013, the Defendant Sean Tiernan pled guilty to Count 1 of the Information charging him with violating the CAN-SPAM Act in violation of Title 18, United States Code, Section 1037(a)(1) and (b)(2)(A). These statutes criminalize the knowing access of a protected computer without authorization and the intentional initiation of the transmission of multiple commercial electronic mail messages from or through such computer(s). During the plea colloquy, the government established that Sean Tiernan participated in a scheme in which other people's social media accounts, and then their physical computers, were infected with malware. This malware caused the infected victim computers to report back to command and control servers which were themselves compromised. Access to these tens of thousands of computers, all without the consent of the true owners of the computers, would then be sold to another individual who would use Tiernan's botnet to forward massive amounts of SPAM messages.

II. SENTENCING CALCULATION

A. Statutory Maximum Sentence

The maximum sentence that may be imposed on the Defendant is imprisonment of up to the three years, a fine of $250,000, and a term of supervised release of no more than 1 year.

B. Sentencing Guidelines Calculation

In reciting the parties' agreement on the appropriate guideline range in this case, the Presentence Report accurate reflects the Defendant's advisory guideline level is 15. Mr. Tiernan has a criminal history category of I. Thus, the sentencing guidelines recommend a sentence of imprisonment of 18-24 months imprisonment.

C. Sentencing Motions

The government will file any appropriate sentencing motions in this matter under seal. If any such motions are filed, this Court, per the procedure set forth above, should consider these motions and rule on them after determining the Sentencing Guideline as set forth above and prior to a determination of the final sentence using the statutory sentencing factors as set forth below.

III. ANALYSIS

This Court must also consider all of the sentencing considerations set forth in Section 3553(a). Those factors include: (1) the nature and circumstances of the offense and the history and characteristics of the Defendant; (2) the need for the sentence imposed to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense; (3) the need to afford adequate deterrence to criminal conduct, and to protect the public from further crimes of the Defendant; (4) the need to provide the Defendant with educational or vocational training, medical care, or other correctional treatment in the most effective manner; (5) the guidelines and policy statements issued by the Sentencing Commission; (6) the need to avoid unwarranted sentence disparities among Defendants with similar records who have been found guilty of similar conduct; and (7) the need to provide restitution to any victims of the offense. 18 U.S.C. § 3553(a).[1] In furtherance of that consideration, the government sets forth certain facts and circumstances pertaining to emphasized factors below.

A. Consideration of the 3553(a) Factors.

[1] Further, the "parsimony provision" of Section 3553(a) states that "[t]he court shall impose a sentence sufficient, but not greater than necessary, to comply with the purposes set forth in paragraph (2) of this subsection." The Third Circuit has held that "district judges are not required by the parsimony provision to routinely state that the sentence imposed is the minimum sentence necessary to achieve the purposes set forth in § 3553(a)(2). . . . '[W]e do not think that the "not greater than necessary" language requires as a general matter that a judge, having explained why a sentence has been chosen, also explain why some lighter sentence is inadequate.'" United States v. Dragon, 471 F.3d 501, 506 (3d Cir. 2006) (quoting United States v. Navedo-Concepcion, 450 F.3d 54, 58 (1st Cir. 2006)).

3553(a)(1)-Nature and Circumstances of the Offense; History and Characteristics of the Defendant

The defendant's scheme in this case touched tens of thousands of people with his fraud. This fraud included the compromising of victims' Facebook accounts and ultimately their computers. The defendant engaged in a complex scheme that involved accessing the Facebook address books of victims' Facebook accounts and the use of those compromised Facebook accounts to send spearphishing messages (carrying malware) to each of the victims' Facebook friends. Once the victims' friends' Facebook accounts were compromised with an unwitting "click" of the message sent by the conspirators, those Facebook accounts' address books would likewise be accessed by the malware, additional spearphishing messages would be sent out, and the malware used by the Defendant and his conspirators would continue to proliferate. Ultimately, the computers which the victims used were compromised with additional malware and became part of the Defendant's "botnet." As such, the conspirators' scheme involved the hijacking of the computing power of tens of thousands of computers belonging to other people without their consent. Furthermore, thousands more likely received unsolicited spam text messages from the computers within the Defendant's botnet.

As reflected in his Guidelines calculation, the Defendant was unjustly enriched by this scheme. As further reflected in his Guidelines calculation, the Defendant possesses advanced and special skills in the field of computer coding. The Defendant committed this offense nearly five years ago at age 23 (at the end of the scheme). Since that time, the Defendant has honed his computing skills, has become well-educated, and is now gainfully and lawfully employed in the field of cyber security.

The Defendant has no criminal history.

3553(a)(2)(A)- Reflect Seriousness of the Offense, Promote Respect for the Law, and to Provide Just Punishment for the Offense

As stated above, the defendant is charged with being involved in a sophisticated cybercrime which affected tens of thousands of people. Although the damage to any victim's computer is difficult to quantify in this case (beyond the invasion of privacy and conversion of property involved with the non-consensual usage of computers by the Defendant and his co-conspirators), the fact remains that the Defendant compromised and turned over the usage of the victim computers to other cybercriminals for money. Thus, the Defendant was unjustly enriched by this scheme.

3553(a)(2)(B)- To afford adequate deterrence to criminal conduct

Cybercrime is an evolving and sometimes complex field. The Internet affords criminals with a level of anonymity that can sometimes be difficult to break through for investigators in order to stop the illegal activity. The Defendant's conviction and sentence in this case will help to send a message that these types of offenses, involving the theft of other's computer functions, will not be tolerated.

IV. CONCLUSION

To be clear, the government recognizes that the guidelines are entirely advisory, and that a district court has discretion to vary from an advisory range, subject only to deferential appellate review for reasonableness. However, a district court must consider the guideline range, see § 3553(a)(4), and is usually well advised to follow the Sentencing Commission's advice, in order to assure fair, proportionate, and uniform sentencing of criminal offenders. See § 3553(a)(6). In this

case, a reasonable sentence should reflect a consideration of the Defendant's initial guidelines calculation set forth by the U.S. Probation Office (18-24 months imprisonment), any motions filed by either party pertaining to a departure from that sentence, and a careful consideration of the statutory sentencing factors as set forth, in part, above.

Respectfully submitted,

SOO C. SONG
Acting United States Attorney

By: s/James T. Kitchen
James T. Kitchen
Assistant U.S. Attorney
PA ID No. 308565
U.S. Attorney's Office
U.S. Post Office & Courthouse
700 Grant Street, Suite 4000
Pittsburgh, PA 15219
Office: 412-644-3500
Jimmy.Kitchen@usdoj.gov